AMENDMENTS TO THE SPECIFICATION

Please replace paragraph [0005] with the following marked-up version of the paragraph:

[0005] One reliable data transport protocol that uses a handshake sequence when challenging a client is known as transmission control protocol (TCP). TCP is used for establishing reliable bidirectional streams, like those used for remote terminal connections (established with telnet or ~~rlogin~~ login utilities). TCP is also used for transferring large amounts of data, for example, with file transfer protocol (FTP) or by connecting to a Web server.

Please replace paragraph [0036] with the following marked-up version of the paragraph:

[0036] Because state information for a remote client is converted into verified information only when a correct response from the peer is received, it is not possible for an attacker to force the conversion from unverified to verified. In particular, because the remote host must know the exact ISN (or other secret shared between the remote client 305 and the local server 310), an attacker will be unable to move state information into the table of verified remote entities 340 without knowledge of the secret. As previously mentioned, since the ISN generated in response to a new connection request needs to be secure, example embodiments provide for using a cryptographically secure hash function (e.g. MD5, SHA, Toeplitz, etc.) with some private key to generate it. Moreover, in the case where the remote entity 305 is an attacker, no response will be received and the state information or TCB within the table of unverified remote entities 335 will eventually time-out.